# NASA Procedural Requirements

**NPR 8715.3C**
Effective Date: March 12, 2008
Expiration Date: March 12, 2013

**COMPLIANCE IS MANDATORY**

Printable Format (PDF)

Request Notification of Change (NASA Only)

## Subject: NASA General Safety Program Requirements

**Responsible Office: Office of Safety and Mission Assurance**



# APPENDIX B. Glossary of Safety and Risk Management Terms

| | |
|---|---|
| Acceptable Risk. | A level of risk, referred to a specific item, system or activity, that, when evaluated with consideration of its associated uncertainty, satisfies pre-established risk criteria. |
| Accident. | A severe perturbation to a mission or program, usually occurring in the form of a sequence of events, that can cause safety adverse consequences, in the form of death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. |
| Accident Prevention. | Methods and procedures used to eliminate the causes that could lead to a accident. |
| Assessment. | Review or audit process, using predetermined methods, that evaluates hardware, software, procedures, technical and programmatic documents, and the adequacy of their implementation. |
| Assurance. | Providing a measure of increased confidence that applicable requirements, processes, and standards are being fulfilled. |

| | |
|---|---|
| Audit. | Formal review to assess compliance with hardware or software requirements, specifications, baselines, safety standards, procedures, instructions, codes, and contractual and licensing requirements. |
| Availability. | Measure of the percentage of time that an item could be used as intended. |
| Buddy System. | An arrangement used when risk of injury is high, where personnel work in pairs, with one person in the pair stationed nearby, not directly exposed to the hazard, to serve as an observer to render assistance if needed. |
| Catastrophic. | (1) A hazard that could result in a mishap causing fatal injury to personnel, and/or loss of one or more major elements of the flight vehicle or ground facility. (2) A condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission. |
| Critical. | A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, or flight hardware. |
| Critical Single Failure Point. | A single item or element, essential to the safe functioning of a system or subsystem, whose failure in a life or mission essential application would cause serious program or mission delays or be hazardous to personnel. |
| Critical Software Command. | A command that either removes a safety inhibit or creates a hazardous condition. |
| Deviation. | An authorization for temporary relief in advance from a specific requirement, requested during the formulation/planning/design stages of a program/project operation to address expected situations. OSHA refers to this as an alternate or supplemental standard. |
| Dominant Root Cause. | Along a chain of events leading to a mishap, the first causal action or failure to act that could have been controlled systemically either by policy/practice/procedure or individual adherence to policy/practice/procedure. |

| | |
|---|---|
| Emergency. | Unintended circumstance bearing clear and present danger to personnel or property which requires an immediate response. |
| Emergency Egress. | The capability for an unassisted crew to exit a vehicle and leave a hazardous situation within a specified amount of time. |
| Emergency Medical. | The capability to respond to illness or injury in order to prevent fatality or permanent disability. This capability includes either an inherent local capability or the timely transfer to a place or vehicle that can provide a similar or higher level of medical care, or both. |
| Emergency Systems. | A set of components (hardware and/or software) used to mitigate or control hazards which present an immediate threat to the crew or crewed spacecraft. Examples include fire suppression systems and extinguishers, emergency breathing devices, and crew escape systems. |
| Exception. | An authorization for permanent relief from a specific requirement and may be requested at any time during the life cycle of a program/project. |
| Exposure. | (1) Vulnerability of a population, property, or other value system to a given activity or hazard; or (2) other measure of the opportunity for failure or mishap events to occur. |
| Facility Hazard Analysis (FHA). | The FHA is a preliminary hazard analysis performed during the planning and decision phases of a facility design and acquisition program. It may later be updated to become the OHA. |
| Factor of Safety (Safety Factor). | Ratio of the design condition to the maximum operating conditions specified during design (see also Safety Margin and Margin of Safety). |
| Fail-Safe. | Ability to sustain a failure and retain the capability to safely terminate or control the operation. |
| Failure. | Inability of a system, subsystem, component, or part to perform its required function within specified limits. |

| | |
|---|---|
| Failure Mode. | Particular way in which a failure can occur, independent of the reason for failure. |
| Failure Modes and Effects Analysis (FMEA). | A bottoms up systematic, inductive, methodical analysis performed to identify and document all identifiable failure modes at a prescribed level and to specify the resultant effect of the modes of failure. It is usually performed to identify critical single failure points in hardware. In relation to formal hazard analyses, FMEA is a subsidiary analysis. |
| Failure Tolerance. | Built-in capability of a system to perform as intended in the presence of specified hardware or software failures. |
| Fault Tree. | A schematic representation resembling an inverted tree that depicts possible sequential events (failures) that may proceed from discrete credible failures to a single undesired final event (failure). A fault tree is created retrogressively from the final event by deductive logic. |
| Fault Tree Analysis. | An analysis that begins with the definition or identification of an undesired event (failure). The fault tree is a symbolic logic diagram showing the cause-effect relationship between a top undesired event (failure) and one or more contributing causes. It is a type of logic tree that is developed by deductive logic from a top undesired event to all sub-events that must occur to cause it. |
| Flight Hardware. | Hardware designed and fabricated for ultimate use in a vehicle intended to fly. |
| Functional Redundancy. | A situation where a dissimilar device provides safety backup rather than relying on multiple identical devices. |
| Ground Support Equipment. | Ground-based equipment used to store, transport, handle, test, check out, service, and control aircraft, launch vehicles, spacecraft, or payloads. |
| Hazard. | A state or a set of conditions, internal or external to a system that has the potential to cause harm. |

| | |
|---|---|
| Hazard Analysis. | Identification and evaluation of existing and potential hazards and the recommended mitigation for the hazard sources found. |
| Hazard Control. | Means of reducing the risk of exposure to a hazard. |
| Hazardous Material. | Defined by law as "a substance or materials in a quantity and form which may pose an unreasonable risk to health and safety or property when transported in commerce" (49 U.S.C S 5102, Transportation of Hazardous Materials; Definitions). The Secretary of Transportation has developed a list of materials that are hazardous which may be found in 49 CFR Part 172.101. Typical hazardous materials are those that may be highly reactive, poisonous, explosive, flammable, combustible, corrosive, radioactive, produce contamination or pollution of the environment, or cause adverse health effects or unsafe conditions. |
| Hazardous Operation/Work Activity. | Hazardous Operation/Work Activity. Any operation or other work activity that, without implementation of proper mitigations, has a high potential to result in loss of life, serious injury to personnel or public, or damage to property due to the material or equipment involved or the nature of the operation/activity itself. . |
| Hazardous Operation Safety Certification. | Certification required for personnel who perform those tasks that potentially have an immediate danger to the individual (death/injury) if not done correctly, could create a danger to other individuals in the immediate area (death or injury), and present a danger to the environment. |
| Imminent Danger. | Condition or practice that could be reasonably expected to cause death or serious physical harm immediately or in the near term. These are classified as Risk Assessment Code (RAC) 1 using the typical NASA risk assessment matrix. |
| Independent Verification and Validation. | Test and evaluation process by an independent third party. |

| | |
|---|---|
| Inhibit. | Design feature that prevents operation of a function. |
| Interlock. | Hardware or software function that prevents succeeding operations when specific conditions are satisfied. |
| Margin of Safety. | Deviation of the actual (operating) factor of safety from the specified factor of safety. Can be expressed as a magnitude or percentage relative to the specified factor of safety. |
| Mission Assurance. | Providing increased confidence that applicable requirements, processes, and standards for the mission are being fulfilled. |
| Mission Critical. | Item or function that must retain its operational capability to assure no mission failure (i.e., for mission success). |
| Mission Success. | Meeting all mission objectives and requirements for performance and safety. |
| NASA Safety Standard (NSS). | A NASA safety document that requires conditions, or the adoption or use of one or more practices, means, methods, operations, or processes reasonably necessary or appropriate to provide for safe employment and places of operation. The document is promulgated by the NASA Office of Safety and Mission Assurance and implemented and enforced by the Center Safety and Mission Assurance organizations. |
| Nuclear Flight Safety Assurance Manager (NFSAM). | The person in the Office of Safety and Mission Assurance responsible for assisting the project offices in meeting the required nuclear launch safety analysis/evaluation. |
| Occupational Safety and Health Administration (OSHA). | The Federal agency which promulgates and enforces workplace safety regulations and guidance. |
| Operability. | As applied to a system, subsystem, component, or device is the capability of performing its specified function(s) including the capability of performing its related support function(s). |

| | |
|---|---|
| Operational Safety. | That portion of the total NASA safety program dealing with safety of personnel and equipment during launch vehicle ground processing, normal industrial and laboratory operations, use of facilities, special high hazard tests and operations, aviation operations, use and handling of hazardous materials and chemicals from a safety viewpoint. |
| Oversight/Insight. | The transition in NASA from a strict compliance-oriented style of management to one which empowers line managers, supervisors, and employees to develop better solutions and processes. |
| Precursor. | An occurrence of one or more events that have significant failure or risk implications. |
| Pressure Vessel. | Any vessel used for the storage or handling of a fluid under positive pressure. A pressure system is an assembly of components under pressure; e.g., vessels, piping, valves, relief devices, pumps, expansion joints, gages. |
| Probabilistic Risk Assessment (PRA). | A PRA is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance in the face of uncertainties. PRA assesses risk metrics and associated uncertainties relating to likelihood and severity of events adverse to safety or mission. |
| Programs. | For the purposes of this NPR the term "programs" shall be interpreted to include programs, projects, and acquisitions. |
| Quality. | The composite of material attributes including performance features and characteristics of a product or service to satisfy a given need. |
| Radiological Control Center (RADCC). | A temporary information clearinghouse established on an as-needed basis to coordinate actions that could be required for mitigation, response, and recovery of an incident involving the launching of nuclear material. |

| | |
|---|---|
| Range Safety. | Application of safety policies, principles, and techniques to ensure the control and containment of flight vehicles to preclude an impact of the vehicle or its pieces outside of predetermined boundaries from an abort which could endanger life or cause property damage. Where the launch range has jurisdiction, prelaunch preparation is included as a safety responsibility. |
| Redundancy. | Use of more than one independent means to accomplish a given function. |
| Reliability. | The probability that a system of hardware, software, and human elements will function as intended over a specified period of time under specified environmental conditions. |
| Reliability Analysis. | An evaluation of reliability of a system or portion thereof. Such analysis usually employs mathematical modeling, directly applicable results of tests on system hardware, estimated reliability figures, and non-statistical engineering estimates to ensure that all known potential sources of unreliability have been evaluated. |
| Residual Risk. | The level of risk that remains after applicable safety-related requirements have been satisfied. In a risk-informed context, such requirements may include measures and provisions intended to reduce risk from above to below an acceptable level. |
| Risk. | The combination of (1) the probability (qualitative or quantitative) of experiencing an undesired event, (2) the consequences, impact, or severity that would occur if the undesired event were to occur and (3) the uncertainties associated with the probability and consequences. |
| Risk Management. | An organized, systematic decision-making process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk to increase the likelihood of achieving project goals. |
| Risk (Safety) Assessment. | Process of qualitative risk categorization or quantitative risk (safety) estimation, followed by the evaluation of risk significance. |

| | |
|---|---|
| Safety. | Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. In a risk-informed context, safety is an overall mission and program condition that provides sufficient assurance that accidents will not result from the mission execution or program implementation, or, if they occur, their consequences will be mitigated. This assurance is established by means of the satisfaction of a combination of deterministic criteria and risk criteria. |
| Safety Analysis. | Generic term for a family of analyses, which includes but is not limited to, preliminary hazard analysis, system (subsystem) hazard analysis, operating hazard analysis, software hazard analysis, sneak circuit, and others. |
| Safety Analysis Report (SAR). | A safety report of considerable detail prepared by or for the program detailing the safety features of a particular system or source. |
| Safety Analysis Summary (SAS). | A brief summary of safety considerations for minor sources; a safety report of less detail than the SAR. |
| Safety Assurance. | Providing confidence that acceptable risk for the safety of personnel, equipment, facilities, and the public during and from the performance of operations is being achieved. |
| Safety Critical. | Term describing any condition, event, operation, process, equipment, or system that could cause or lead to severe injury, major damage, or mission failure if performed or built improperly, or allowed to remain uncorrected. |
| Safety Critical Function. | A system, equipment, or facility function or process that, by not performing as intended, causes a safety critical condition or event. |
| Safety Device. | A device that is part of a system, subsystem, or equipment that will reduce or make controllable hazards which cannot be otherwise eliminated through design selection. |

| | |
|---|---|
| Safety Evaluation Report (SER). | A safety report prepared by the INSRP detailing the INSRP's assessment of the nuclear safety of a particular source or system based upon INSRP's evaluation of the program-supplied SAR and other pertinent data. |
| Safety Margin. | Difference between as-built factor of safety and the ratio of actual operating conditions to the maximum operating conditions specified during design. |
| Safety Oversight. | Maintaining functional awareness of program activities on a real-time basis to ensure risk acceptability. |
| Safety Program. | The implementation of a formal comprehensive set of safety procedures, tasks, and activities to meet safety requirements, goals, and objectives. |
| Serious. | When used with "hazard," "violation," or "condition," denotes there is a substantial probability that death or serious physical harm could result. |
| Single Failure Point. | An independent element of a system (hardware, software, or human) the failure of which would result in loss of objectives, hardware, or crew. |
| Software Hazard Analysis. | Identification and verification of adequate software controls and inhibits; and the identification, analysis, and elimination of discrepancies relating to safety critical command and control functions. |
| System Safety. | Application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. |
| System Safety Manager. | A designated management person who, qualified by training and/or experience, is responsible to ensure accomplishment of system safety tasks. |
| Vacuum System. | An assembly of components under vacuum, including vessels, piping, valves, relief devices, pumps, expansion joints, gages, and others. |

| | |
|---|---|
| Validation. | (1) An evaluation technique to support or corroborate safety requirements to ensure necessary functions are complete and traceable; or (2) the process of evaluating software at the end of the software development process to ensure compliance with software requirements. |
| Variance. | An authorization for temporary relief in advance from a specific requirement and is requested during the formulation/planning/design stages of a program/project operation to address expected situations. |
| Verification (Software). | (1) The process of determining whether the products of a given phase of the software development cycle fulfill the requirements established during the previous phase (see also validation); or (2) formal proof of program correctness; or (3) the act of reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether items, processes, services, or documents conform to specified requirements. |
| Waiver. | A variance that authorizes departure from a specific safety requirement where a certain level of risk has been documented and accepted. |

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | ALL |

| NODIS Library | Program Management(8000s) | Search |

**DISTRIBUTION:**
**NODIS**